
desať prikázaní
bezpečného
elektronického podnikania

obsah

Tento dokument je určený predovšetkým IT managerom, bezpečnostným správcom a ostatným bezpečnostným profesionálom v strategických pozíciách.

Uvedené informácie majú za úlohu všeobecne priblížiť oblasť bezpečnosti IT. Sú upravené tak, aby boli prístupné aj laikom a poskytli primeranú podporu každému, kto si myslí, že bezpečnostné otázky má riešiť predovšetkým management organizácie.

Ba čo viac, tento materiál by si mal prečítať každý člen riadiaceho tímu, ktorý chce, aby jeho organizácia bola favoritom v novom ekonomickom prostredí.

Tento dokument bol vytvorený v Protect Data, v skupine, ktorá zaujíma vedúce miesto v oblasti bezpečnosti IT. Našim cieľom je čiastočne aj náš vlastný prospech – máme snahu predstaviť naše bezpečnostné riešenia.

Na druhej strane, najväčší prínos tohoto dokumentu je v tom, že ilustruje spôsob, ako dôvera a spoľahlivosť buduje základy, na ktorých stojí nový model podnikania a poskytovania služieb.

Nový prístup k bezpečnosti IT

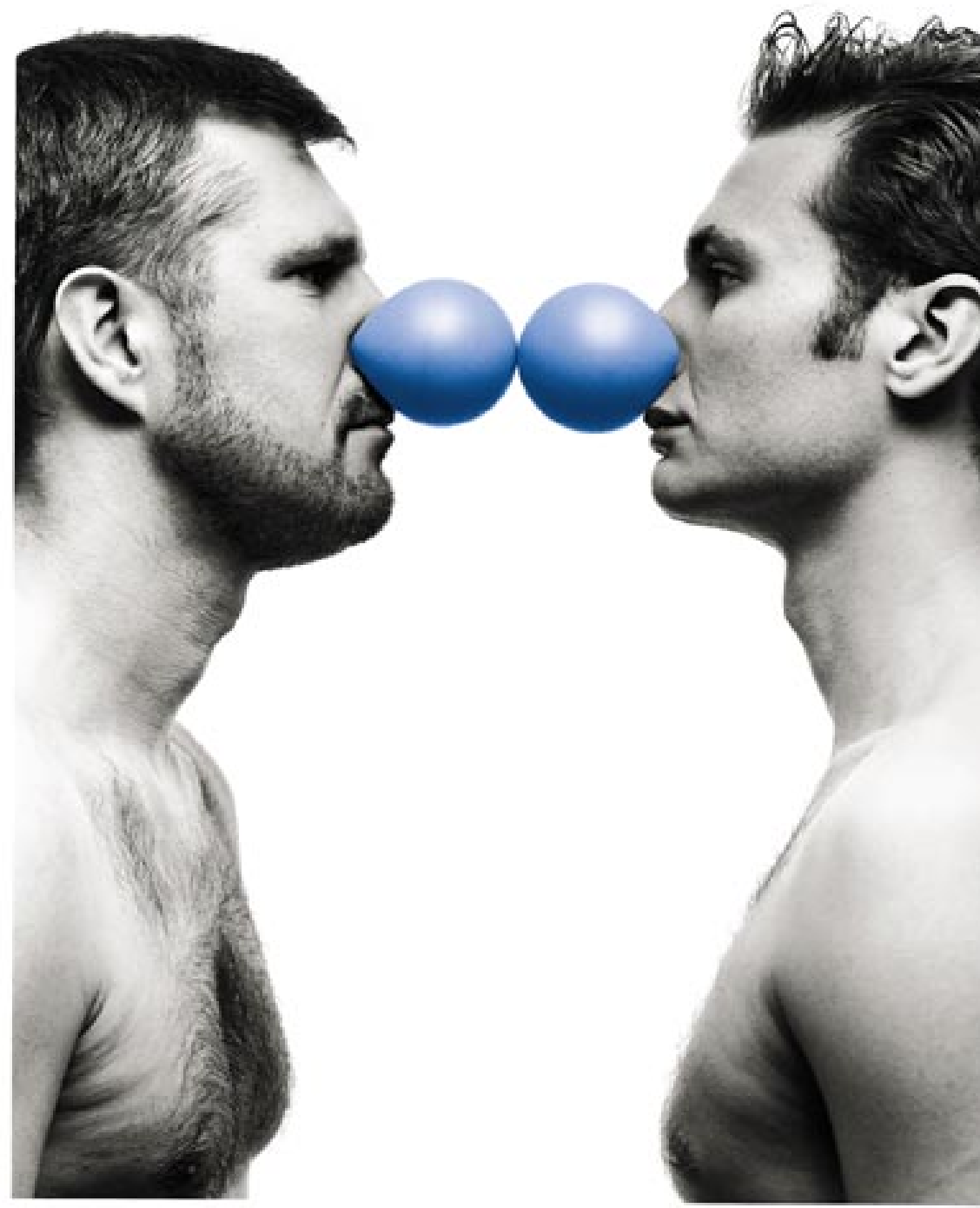
Revolúcia v oblasti IT (informačné technológie) ovplyvňuje čoraz viac oblastí podnikania a čoraz viac sa presadzuje nový prístup k bezpečnosti IS (informačné systémy). Bezpečnosť dnes už nie je len o tom, ako vymknúť nežiadúcich návštevníkov, ale o tom, ako vpustiť dnu tých pozvaných a žiadaných: potencionálnych zákazníkov, dodávateľov, zamestnancov a ďalšie skupiny. Od samotných počiatkov podnikanie spočívalo na dôvere a vytvorení dôveryhodného prostredia. Najväčšou výzvou dneška je preniesť tieto hodnoty do elektronického sveta. Zároveň to kladie celú sériu nových požiadaviek nielen na existujúce pracovné metódy, ale aj na celkové prostredie IT.

Na prvý pohľad sa zdá, že nejde o nič iného, ako nahradiť krok za krokom klasický, na papierových dokumentov založený proces procesom elektronickým, s dodržaním prinajmenej rovnakej, ak nie vyššej bezpečnosti. V skutočnosti však skôr ide o vybudovanie tzv. business-critical systémov.

Pri transformácii business-critical materiálov z papierovej formy do formy elektronickej, musíme byť schopní klásť na informácie a ich hodnovernosť rovnaké, alebo ešte vyššie nároky. Obrovský objem informácií znamená, že ich autenticita sa musí dať overiť veľmi rýchlo a automaticky, bez kladenia nových požiadaviek na technickú úroveň a znalosti koncového užívateľa.

To, čo bolo bezpečne uzamknuté včera, dnes môže byť voľne prístupné na serveri. To, čo sme podpísali a zalepili do obálky včera, je dnes podpísané elektronickým podpisom s cieľom prepožičať dokumentu tú istú hladinu kredibility. Pri transformácii z fyzického do elektronického sveta môžeme dokonca klásť vyššie požiadavky na prínosy z podnikania a požadovanú hladinu bezpečnosti.

Bezpečnosť IT sa stala základnou požiadavkou podnikania v novej ekonomickej ére. Prináša so sebou úplne nové služby, zvyšuje konkurencieschopnosť, prináša nových zákazníkov a dramaticky zvyšuje geografické pokrytie. Dovoľte nám vysvetliť, ako sa to deje.



bezpečnosť IT môžeme sumarizovať v jednom slove: dôvera

Ak existuje jediné slovo sumarizujúce výhody elektronického podnikania, je to dôvera. Bez ohľadu na typ ponúkanej elektronickej služby, základom je vytvorenie solídneho prostredia pre dôveru.

Zákazník, ktorý chce používať Internet banku, musí mať absolútnu dôveru v bankový bezpečnostný systém. Musí si byť istý, že nikto iný nemôže získať prístup na jeho bankový účet
a uskutočniť peňažný transfer. Už len myšlienka o možnosti kompromitácie jeho prístupu pravdepodobne povedie k tomu, že zmení banku.

Dôvera sa aplikuje aj na dokumenty, ktoré niekto zverejnil. Čo by sa asi stalo, keby niekto sprístupnil novú web stránku a začal na nej uverejňovať nepravdivé tlačové správy? Presne to sa stalo na Wall Street, keď niekto začal distribuovať falošné informácie o cenách akcií na burze využívajúc nepravý server. Vyhnalo to hore dočasne niektoré ceny akcií, avšak dostatočne dlho na to, aby niekto pri ich predaji zhrabol mimoriadny zisk.

Ak by verejnosť dala svoju dôveru falošným informáciám, môže to mať aj oveľa vážnejšie dôsledky - hlavne v strate dôvery voči danej organizácii a jej značke. A značka niekedy pre firmu predstavuje oveľa väčšiu hodnotu ako cena jej akcií na burze.

porovnanie prínosov a nákladov podnikania

Vytváranie služieb poskytovaných cez rozhranie www, prilákanie zákazníkov a vytváranie obchodných vzťahov vyžaduje podstatné investície.

Citlivý vzťah zákazníka k Internet banke je toho žiarivým príkladom. Ak sa rozšíri chýr, že zákazník prišiel o všetky svoje peniaze v banke fungujúcej cez web, dôvera sa okamžite vyparí a nastane prudký odliv zákazníkov. V takomto prípade, databáza zákazníkov, ktorá sa budovala niekoľko rokov sa stane bezcennou v priebehu niekoľkých dní.

V porovnaní s možnými stratami v dôsledku toho, že sa niečo pokazilo, investície do zabezpečenia systému pre podnikanie sú relatívne malou investíciou. V ideálnom prípade, bezpečnosť sa vytvára zároveň s budovaním služieb založených na webe. Najekonomickejším riešením je, ak sa investície naplánujú už vo fáze plánovania systému ako takého a bezpečnosť IT sa inkorporuje do systému hneď od začiatku.

Ak by sa čakalo až do momentu, kedy vznikne problém, riešenie by mohlo byť príliš drahé, ťažko uskutočniteľné – prípadne by bolo úplne nemožné odstrániť negatívne dôsledky. Vytváranie dobrých vzťahov so zákazníkmi je dlhodobý proces, ich zničenie môže byť záležitosťou sekúnd.

motivácia vo vašej organizácii

Každopádne je viac aktívnych, ako pasívnych argumentov pre investovanie do zabezpečenia elektronického podnikania hneď od začiatku.

Tri najzrejmejšie požiadavky v podnikaní sú zvýšenie profitability, vytvorenie náskoku pred konkurenciou a vytvorenie silných obchodných vzťahov. Toto nie je nič prevratne nového, ale prostriedky pre dosahovanie týchto cieľov v novom ekonomickom prostredí sú nové. Či už to bude znamenať otvorenie nových trhových priestorov, ktoré predtým boli nedostupné a príliš ďaleko, alebo zníženie nákladov na služby poskytované zákazníkom. Základným princípom ostáva: nechať zákazníkov viac konať - jednoduchšie a rýchlejšie, čím sa spoločnosti uvoľnia zdroje na to, aby mohla slúžiť viacerým zákazníkom a ponúknuť kvalitnejšie služby.

Je rozumnejšie implementovať inteligentný systém, schopný preberať objednávky a zasielať ich ďalej dodávateľom, ako zamestnať dodatočných desať ľudí.

Premysleným riešením je často aj efektívny konkurečný nástroj. Ak prostredníctvom bezpečnostného riešenia viem ponúknuť zákazníkovi niečo navyše, získavam náskok pred konkurenciou, ktorá takéto riešenie nemá.

Príkladom takého riešenia môže byť povolenie prístupu zákazníkovi pre skontrolovanie stavu objednávky, pričom konkurencia takúto službu poskytovať nemôže. Je to ďalej aj spôsob, ako sa priblížit k zákazníkovi a vytvoriť silnejšiu podnikateľskú väzbu.

Spoločnosti s veľkým počtom obchodných partnerov a dealerov im môžu povoliť prístup a kontrolu objednávok a ich stav, ba dokonca aj priamo zadávať objednávky. Príkladom môže byť automobilová spoločnosť, resp. dealer, napr.Volvo alebo Škoda, ktorý umožní týmto spôsobom špecifikovať model a vybavenie pred samotným zadaním objednávky. Druhým príkladom je IKEA, kde zákazníci majú povolený prístup k informáciám o tom, čo je na sklade a zároveň majú možnosť hneď umiestniť objednávku bez toho, aby čakali na telefóne, kým sa ich ujme niektorý predajca. Ponúknutie produktu cez web tiež vedie k zníženiu časovej náročnosti marketingu v porovnaní s normálnym obchodným predajom.

Napríklad, máte obchodný nápad, ktorý nie je však realizovateľný vo vašom malom meste vzhľadom na limitovaný trhový priestor. Ak však ste schopný ponúknuť takýto produkt cez web, situácia môže vyzerať úplne inak a nápad bude realizovateľný. Takto dosiahnete spoločnosti, o ktorých ste včera ani nevedeli, že existujú, alebo boli mimo váš dosah. Je ťažko povedať, kde na zemi sa bude nachádzať váš trhový priestor, ale pri obchodovaní cez Internet pre vás nebudú existovať žiadne hranice.

Nové ekonomické prostredie znamená čoraz viac vytvárenie vzťahov cez neosobné médium a ich dlhodobé budovanie. Kľúčom k budovaniu tvalých hodnotných obchodných vzťahov je neustále rástúca vzájomná výmena kvalitných informácií. Zákazník poskytuje informácie týkajúce sa jeho požiadaviek a nárokov, na oplátku získava informácie upravené podľa jeho požiadaviek. To je zároveň dôvodom neustále rastúcich nárokov na vytvorenie efektívneho informačného systému založeného na vzájomnej dôvere.

Správa Forrester Research odhaduje, že elektronické transakcie dosiahnu úroveň len v USA 1,300 miárd dolárov v roku 2003! Tieto čísla sú ohromujúce. Ďalšie inštitúcie predpovedajú, že organizácie, ktoré nebudú schopné zadaptovať svoje podnikanie pre svet elektronického obchodovania, nebudú na trhu schopné konkurencie.

predpovedanie rizika

Je zrejmé, že každý sa bude pokúšať uskutočňovať elektronické transakcie a podnikanie s minimálnym možným rizikom. Potrebujeme vedieť, či nepúšťame našich zákazníkov príliš hlboko do systému. A zároveň si musíme byť istý, že uskutočňovanie transakcií nás nevystaví rizikám, ktoré by neskôr mohli viesť k nepríjmeným prekvapeniam.

Elektronické podnikanie teda kladie vysoké požiadavky na bezpečné a funkčné riešenia IT. Jednou stránkou je fukcionalita IT, druhou stránkou je racionálnosť využívania takéhoto systému.

Fundamentálnou otázkou ostáva, čo by spoločnosť stálo, keby niekto poškodil elektronické podnikanie spoločnosti.

Jedna dobre známa stránka na webe tvrdí, že by sa nič strašné pri podobnom poškodení bezpečnosti IT systému nestalo. Dávajú prednosť riziku akceptovania nekorektnej objednávky. Podľa nich omyl nebude stáť priveľa, nakoľko predávajú tovar s relatívne nízkou hodnotou. Ak by však

“Nové ekonomické prostredie znamená čoraz viac vytvárenie a budovanie vzťahov na dlhé obdobie”

niekto prenikol do systému a poslal milión neoprávnených objednávok, ich názor by sa pravdepodobne zmenil. Alternatívou by bolo telefonicky overovať každú objednávku, avšak takýto spôsob obchodovania by bol neúmerne náročný na čas.

Zatiaľ sme hovorili len o omyle, ale problém môže zapríčiniť obchodný konkurent úmyselne, alebo aj nevedomosť a zneužitie. V jednej školskej triede v Štokholme niekto objednal cestovné lístky cez web stránku cestovnej agentúry v hodnote približne 7.500 USD. Prirodzene účet prišiel ako patričný šok pre rodičov. Kedže na účte nebola ani zmienka o možnosti a termíne zrušenia objednávky, rodičia museli zavolať agentúru a požiadať o zrušenie objednávky. Akú dôveru však budú mať zákazníci v systém, ktorý nie je dostatočne chránený? Bez patričnej ochrany sa ktokoľvek môže cez Internet prihlásiť na stránku a v mene hocikoho objednať čokoľvek.

Internet je dnes prístupný kdekoľvek, na školách, letiskách, v kaviarňach a je prakticky nemožné vystopovať niekoho, kto sa pripájal z takýchto verejných miest.

Ked začiatkom roku 2000 bol “bombardovaný” internetový portál Yahoo, pochopiteľne došlo k zníženiu produktivity tejto stránky. Omnoho väčšou stratou bola však strata kredibility a v tomto prípade hovoríme o miliardách dolárov. Skúsenosti Yahoo sú excelentným príkladom, prečo je potrebné analyzovať riziká a zabezpečiť integrovanú bezpečnostnú infraštruktúru podnikateľských aktivít hneď od začiatku.

aké rozmery nadobúda e-bezpečnosť?

Je dôležité ustanoviť rovnováhu medzi podnikateľskými aktivitami a stupňom požadovanej bezpečnosti pre jednotlivé transakcie. Za normálnych okolností sa to deje prepočítaním nielen finančných výnosov, ale aj strát, ktoré by nastali, ak by sa niečo zlého prihodilo. Bezpečnostný systém môže byť dimenzovaný v súlade s hodnotou jednotlivých transakcií a stupňom dôvery vyžadovaným pre jednotlivé služby.

Najjednoduchším príkladom je internetovská domovská stránka, ktorá ponúka len základné informácie. Je zrejmé, že pri ponúkaní základných informácií, akými sú napr. kontaktné adresy, nie je potrebné nasadiť najvyššiu hladinu bezpečnosti.

Opačná situácia nastáva, akonáhle povolíme uskutočňovanie transakcií. Objednávanie, napr. kníh, bude vyžadovať niektorú zo základných hladín bezpečnosti. Avšak poskytnutie možnosti objednať si kamión Volvo posunie požiadavky na bezpečnosť podstatne vyššie. Základnou otázkou zostáva: “ Aké sú náklady na transakciu?”. Ešte lepšie vyjadrené, koľko stratíme, ak transakcia zlyhá a neprebehne korektne? Napr. koľko by nás stálo, ak by sme poslali desať kamiónov Volvo špeciálne nastriekaných a označených logom zákazníkovi, ktorý ani nevie, že v jeho mene bola vystavená nejaká objednávka?

Hodnota je vitálnou pri určovaní investícii do bezpečnosti IT. Dôležitým faktom je aj poznatok, že sa jedná o investíciu - a nie náklady.

Je veľmi dôležité vybudovať trvalú dôveru v obchodnú značku spoločnosti. Vo fungujúcom systéme, veľa malých úspešných a fungujúcich transakcií vytvára bázu pre veľký objem transakcií, čím sa ďalej posilňuje dôvera a dosahujú sa podnikateľské ciele.

prvky v zákulisí bezpečnostnej politiky IT

Ako pre všetky ostatné oblasti podnikania, aj pre oblasť IT bezpečnosti sú determinujúcimi samotné ciele podnikania. Existujú štyri základné kamene definujúce a ovplyvňujúce bezpečnosť existujúcu vo vnútri organizácie:

- Samotné ciele podnikania
- Úroveň technickej podpory v oblasti IT, ktorú má organizácia k dispozícii
- Zákony a predpisy regulujúce podnikanie
- Etika a morálka

Tieto štyri základné kamene silne ovplyvňujú hladinu bezpečnosti v konkrétnej organizácii. Najdôležitejšie je určenie rizík, ktorým je organizácia vystavená. Následne je potrebné načrtnúť pravidlá a postupy, ako sa s týmito rizikami vyrovnať.

“Najdôležitejšie je dosiahnutie rovnováhy medzi potrebnou úrovňou bezpečnosti a typom požadovanej transakcie”

Tieto pravidlá a postupy vytvárajú to, čo my nazývame bezpečnostná politika IT. Ak chceme vytvoriť korektnú bezpečnostnú politku, musíme najprv vykonať analýzu opierajúcu sa o spomenuté štyri základné kamene.

V prvom rade, aké sú očakávania na úrovni top managementu pokiaľ ide o ciele podnikania, aké sú hrozby, napr. konkurencia, vývoj, politika a pod.?

Po druhé, aké sú úlohy pre technickú podporu IT pre oblasť finančných systémov, podpory predaja a ostatných systémov pre uskutočňovanie transakcií? Ďalej su tu právne a legislatívne aspekty. Aké záväzky má organizácia vzhľadom na platné zákony a predpisy? Príkladom môžu byť predpisy o ochrane osobných informácií, kolektívnych dohôd a záväzkov, predpisy o archivácii dát a pod.

Na záver tu máme otázky morálky a etiky, kde patrí aj školenie personálu, obsahuje etické a morálne aspekty vo vzťahu k Internetu a jeho využívania. Kultúrne dedičstvo v danej konkrétnej organizácie môže byť pre formuláciu takýchto etických princípov veľmi dôležité.

Opierajúc sa o tieto štyri základné kamene sa uskutoční analýza existujúcich rizík. Dôležitým je aj zhodnotenie rizík z finančného hľadiska. Napr. čo nás bude stáť, ak prebehne scenár X, alebo sabotáž Y?

ohodnotenie rizík

Prednedávnom bola veľká švédska priemyselná firma kompletne paralyzovaná na niekoľko hodín následkom vírusu vo svojej sieti. Po prerušení sieť nebola ešte dlho extenzívne využitá. Ľudia nevedeli, čo robiť. Táto nevedomosť prispela k zvýšeniu strát.

Straty môžu byť priamym dôsledkom výpadku produkcie, ale aj vo forme extra úsilia a práce pre personál, následne vo forme nadčasov a dodatočných nákladov. Okrem toho sa stretávame s nekvantifikovateľnými stratami vo forme stresu individuálnych pracovníkov.

Analýza rizík by mala vyústiť do finálnych vyhlásení ako: „Toto môžeme akceptovať.“ „Toto nemôžeme akceptovať.“ „S týmto musíme niečo urobiť.“

načrtnutie bezpečnostnej politiky IT

Bezpečnostná politika je formulovaná na základe analýzy existujúcich rizík. Myšlienkou je vyjadrenie všeobecného cieľa a zámeru organizácie. Bezpečnostná politika kladie základy pre súbor opatrení, na základe ktorých sa tvorí rozpočet pre bezpečnosti IT a určujú sa primerané zdroje. Bezpečnostná politka má svoju obdobu a podobá sa ostatným typom politiky organizácie, ako napr. personálna politika, politika pre vyplácanie miezd a pod.

Bezpečnostná politika musí vyjadrovať spôsob, akým organizácia pristupuje k rizikám, čo vyžaduje od svojich zamestnancov a vedenia na rôznych úrovniach. Musí pevne
a jednoznačne určovať, čo je dovolené a čo nie je dovolené.

Bezpečnostná politika môže obsahovať niekoľko prehlásení tohto typu:

- Ak ktokoľvek v organizácii má podozrenie na výskyt vírusu, musí zavolať na toto telefónne číslo a kontaktovať technickú podporu s cieľom získať ďalšie inštrukcie
- Všetci vzdialení užívatelia pristupujúci do siete organizácie musia podstúpiť overovací proces, ktorý jednoznačne zaručí autentifikáciu toho, kto sa hlási do siete
- Každá informácia označená ako „Interná“ musí byť pred odoslaním zašifrovaná

konkrétne pravidlá sú formulované na základe bezpečnostnej politiky

Akonáhle je vytvorená bezpečnostná politka, nasleduje vytvorenie súboru pravidiel a opatrení. Napr. vo forme bezpečnostného manuálu obsahujúceho direktívy v prípade bezpečnostného incidentu. Ak niekto zavolá bezpečnostné oddelenie a povie „máme vírus“, musí byť spustený systém krokov hovoriaci „najprv urob toto, potom toto a nakoniec toto“.

Tento súbor krokov ovšem nie je statický, ale je dynamickým fenoménom podliehajúcim vývojovým zmenám a úpravám. Nejedná sa teda o systém pre každého, ale každý si musí byť vedomý krokov, za ktoré je zodpovedný.

Je zároveň veľmi dôležité uskutočniť praktické testovanie, aby sa otestovali protiopatrenia určené na vykonanie jednotlivými pracovníkmi.

Pri vytváraní bezpečnostného manuálu a pripomenutí si všetkých potrebných oblastí, ktoré treba brať do úvahy, výbornou pomôckou môže

pár slov o zákonoch a dohodách, etike a morálke

Bezpečnostná ochrana organizácie by nemala vychádzať čiste z technokratického pohľadu, ale mala by brať do úvahy aj iné pohľady, ako napr. personálne, organizačnú kultúru a pod.

Požiadavky na bezpečnosť môžu priniesť zásadné zmeny jednak v štruktúre organizácie samotnej, ale aj pre jednotlivých zamestnancov.

Už dnes existuje celý rad nariadení a noriem vzťahujúcich sa na oblasť IT a je pochopiteľné, že v prípade kontroly a inšpekcie, organizácia má záujem dokázať, že tieto predpisy a nariadenia dodržiava.

Ak chcete dodržiavať zákony, musíte ich v prvom rade poznať. Ako príklad uvedieme, že organizácia narábajúca so zdravotnými dátami v elektronickej forme, musí mať na to príslušnú licenciu.

Vo veľa krajinách existujú nariadenia určujúce, či organizácia má alebo nemá právo kontrolovať osobné emaily zamestnancov, v iných krajinách toto môže byť predmetom špecifickej zmluvy medzi zamestnávateľom a zamestnancom.

je v poriadku, ak v zamestnaní surfujeme na sieti?

Ak pokračujeme s otázkami ohľadne etiky a morálky, vyvstáva otázka, či je korektné, ak dovolíme zamestnancom surfovať po Internete v pracovnom čase a navštevovať stránky, ktoré obsahujú menej „žiadúci“ obsah. Môže sa jednať o relatívne neškodnú záležitosť, ako sú napr. stránky určené pre fanúšikov dostihov. Ale aj o relatívne veľmi nepríjemné záležitosti, ako keď napr. jedna vážená švédska firma našla pri rutinnom prehliadaní počítačov vo svoje sieti stovky obrázkov detskej pornografie. Ďalšou otázkou je - dovolíte zamestnancom robiť I-banking z pracoviska?

V horšom prípade intenzívne surfovanie vedie k preťaženiu siete organizácie. Rizikom sa stáva, že ľudia robiaci dôležité rozhodnutia sa nebudú môcť v danom čase dostať k vitálnym informáciám. To môže zásadne ovplyvniť hodnotu akcií firmy na burze.

Problémy týkajúce sa zamestnancov musia byť samozrejme riešené v spolupráci buď s odbormi, alebo s inými predstaviteľmi zamestnancov, čo by malo prispieť k vytvoreniu otvoreného a konštruktívneho dialógu. Zamestnanci sú najdôležitejšími aktívami spoločnosti a musia k nej byť lojálni. Na druhej strane, organizácia si musí uvedomiť, že bezpečnosť a ochrana je dôležitá zvonka, ale rovnako aj zvnútra.

zisťovanie a prevencia neautorizovaného prístupu

Na jednej strane je snaha o vytvorenie systému maximálne otvoreného a prístupného užívateľom a zákazníkom. Na druhej strane toho istého procesu je nevyhnutnosť zabudovať spôsoby ochrany pred neautorizovaným používaním systému, skompromitovaním IT systému a snahám o sabotáž. Aj keď všeobecné podvedomie týkajúce sa bezpečnostných otázok je neustále silnejšie, naďalej existuje veľa organizácií, ktorých senzitívne informácie ležia nechránené a voľne dostupné. Príčiny sú rôzne, od neznalosti problematiky a existujúcich rizík, cez neznalosť metód umožňujúcich získanie existujúcich hesiel, až po zlú konfiguráciu systémov a existenciu tzv. zadných dvierok do systémov.

začalo to externou ochranou

Vo svete, kde organizácie boli viac menej v terminológii počítačov izolované od zákazníkov a klientov, bezpečnosť IT sa týkala hlavne externej ochrany vo forme alarmov, zablokovania a prekážok. Samozrejme, v omnoho intezívnejšie integrovanom prostredí logickým centrom pozornosti boli firewally. Zintenzívnenie prepojenia s vonkajším svetom postupne prenieslo koncentráciu pozornosti na kontrolu vírusov, šifrovanie a pod.

Z pohľadu organizácie je prijateľnejšie presvedčenie, že útok a zneužitie systému prichádza zvonka. Avšak skúsenosť nám hovorí, že väčšina útokov prichádza zvnútra. Je pre nás prirodzené predpokladať, že naši zamestnanci sú nám lojálni, ale zmeny v organizácii často vedú k opačnej situácii. Príčinou zneužitia systémov môže byť aj nedostatok poznatkov. Z hľadiska ochrany systému je preto potrebný komplexný pohľad na problematiku zahrňujúci alternatívu ohrozenia zvonka aj zvnútra.

báza pre rozhodovanie o investíciách do bezpečnosti

V minulosti neboli k dispozícii žiadne mierky a etalóny na zhodnotenie stavu bezpečnosti. Dnes je však k dispozícii celý rad riešení určených na vyhľadávanie slabých miest v systémoch, vyvolanie alarmu a registrovanie nepovolených činností. Slúžia bezpečnostnému manažérovi v organizácii prostredníctvom komplexných správ o neautorizovaných prístupoch a pokusoch, útokoch, vniknutiach a snahách o manipuláciu systému resp. informácií v ňom uložených. Takáto dokumentácia je významným nástrojom pre proces rozhodovania managementu ohľadne zvyšovania úrovne ochrany a investícií na to potrebných. Spoločným názvom pre tento typ programov je Bezpečnostný skener (Security Scanner) resp. Detekcia vniknutia (Intrusion Detection) a ich prvoradou úlohou je vyhľadávanie a prioritizácia slabých miest v systéme.

“Otvorenie systému do maximálnej možnej miery pre užívateľov a zákaznikov súčasne vyžaduje zabudovanie účinných metód ochrany”

šesť základných funkcií

1. identita

Elektronická identifikácia nesie označenie autentifikácia. Autentifikácia sa môže vzťahovať na fyzickú alebo právnickú osobu, ale tiež na server, funkciu, alebo službu. Autentifikácia vyúsťuje do potvrdenia bezpečnej identifikácie a overuje, že osoba pripojená na opačnom konci cez Internet je naozaj tou, za ktorú sa vydáva a vice versa. Na úplne základnej hladine sa môže jednať o zaslanie emailu určitej osobe s vedomím, že daná správa sa naozaj dostane k tej pravej osobe, resp. že daný odosielateľ je naozaj osobou, ktorá túto správu poslala.

Ak nie je možné spoľahlivo určiť identitu druhej strany, nie je možné s ňou podnikať. Identifikácia je teda základnou podmienkou pre vykonávanie elektronického obchodovania. Dokonca aj keby daná informácia bola zašifrovaná, nie je to postačujúce na overenie identity odosielateľa alebo autenticity samotnej informácie.

Užívatelia sa stretávaju s autentifikáciou pri Internet bankingu kde sa musia identifikovať ako majitelia účtu a zákazníci, používajúci napr. generátor hesiel (token) alebo čipovú kartu. Následne banka vie, že do systému sa hlási oprávnená osoba. Na druhej strane zákazník si je istý tým, ze sa pripája na správnu banku.

V komplikovanejších prípadoch, napr, pri výmene informácií medzi organizáciami, užívateľ si musí byť istý, že komunikuje s korektným serverom a môže napr. umiestniť objednávku, vystaviť faktúru alebo uskutočniť nejakú inú elektronickú operáciu.

2. kontrola prístupu determinuje privilégia užívateľa

Akonáhle je overená identita, ďalšou otázkou je, akými oprávneniami disponuje užívateľ hlásiaci sa do systému a vyžadujúci cez sieť rôzne služby a zdroje.

Kontrola prístupu k rôznym typom informácií alebo zdrojov je teda tiež fundamentálnou bezpečnostnou otázkou. Danou informáciou môže byť

prípadne plné oprávnenie pre finančný, účtovný alebo skladový systém. Kontrola prístupu sa môže opierať aj o funkciu resp. postavenie v organizácii.

Ak použijeme ako príklad banku, tak aj v prípade, že banka už vie, s kým komunikuje, musí zabezpečiť, aby zákazník mal prístup na správny účet a služby, umožňujúce napr. transfer peňazí, alebo nákup akcií na burze.

V prípade elektronického podnikania organizácie kontrolujú, aký typ služby je pre daného zákazníka alebo dodávateľa prístupný cez web.

Kontrola prístupu zahrňuje zadefinovanie pravidiel determinujúcich, kto má za akých okolností prístup k daným zdrojom. Takéto podmienky môžu existovať aj vo forme časových limitov, napr. konzultant bude mať právo pripojiť sa na sieť organizácie len počas pracovných hodín. Na druhej strane, zamestnanec môže mať pridelené oprávnenie pripájať sa na sieť počas 24 hod. denne, ak pracuje z domu a používa Internet.

3. dôvernosť v preklade znamená, že nedochádza k neautorizovanému načítaniu informácií

Dôvernosť teda znamená, že neautorizovaný subjekt nemôže získať informáciou, ktorá je v systéme uložená alebo prenášaná. Znamená to chrániť informáciu tak, aby si ju nikto nepovolaný nemohol prečítať. Typickým príkladom je šifrovanie elektronickej pošty. Na Internete je všetka pošta, pokiaľ nie je nejakým spôsobom chránená, v podstate ľahko prístupná.

Dôvernosť samozrejme znamená aj ochranu informácií uložených na PC a pevných diskoch zamestnancov, resp. na serveroch organizácie. Vzhľadom na objem a povahu senzitívnych informácii často uložených na moderných laptopoch, ani prenosné počítače nemožno ponechať nezabezpečené.

Pri pripojení užívateľa na Internet-banku je komunikácia medzi nimi zašifrovaná. Vyplýva to z potreby chrániť integritu privátnych dát, ako aj z nutnosti rešpektovať pravidlá a zákony týkajúce sa bankovníctva.

V praxi to vyzerá tak, že komunikácia medzi web serverom banky a prehliadačom zákazníka je zašifrovaná. Medzi zákazníkom a bankou sa vytváraná chránený tunel. Samozrejme, deje sa to transparentne, t.j. pre zákazníka je táto operácia neviditeľná.

4. integrita v preklade znamená, že informácia nie je porušená

Integrita znamená, že správa alebo prenášané, či uložené súbory neboli zmenené. Ak napr. správa znie“ „Kúp 500 akcií Ericssonu“, je dôležité, aby v správe nepribudla jedna nula navyše. Integritu možno dosiahnuť len tak, že sa pomocou kontrolnej funkcie sleduje, či došlo k nejakej zmene v správe, uloženom súbore alebo v bankovej transakcii.

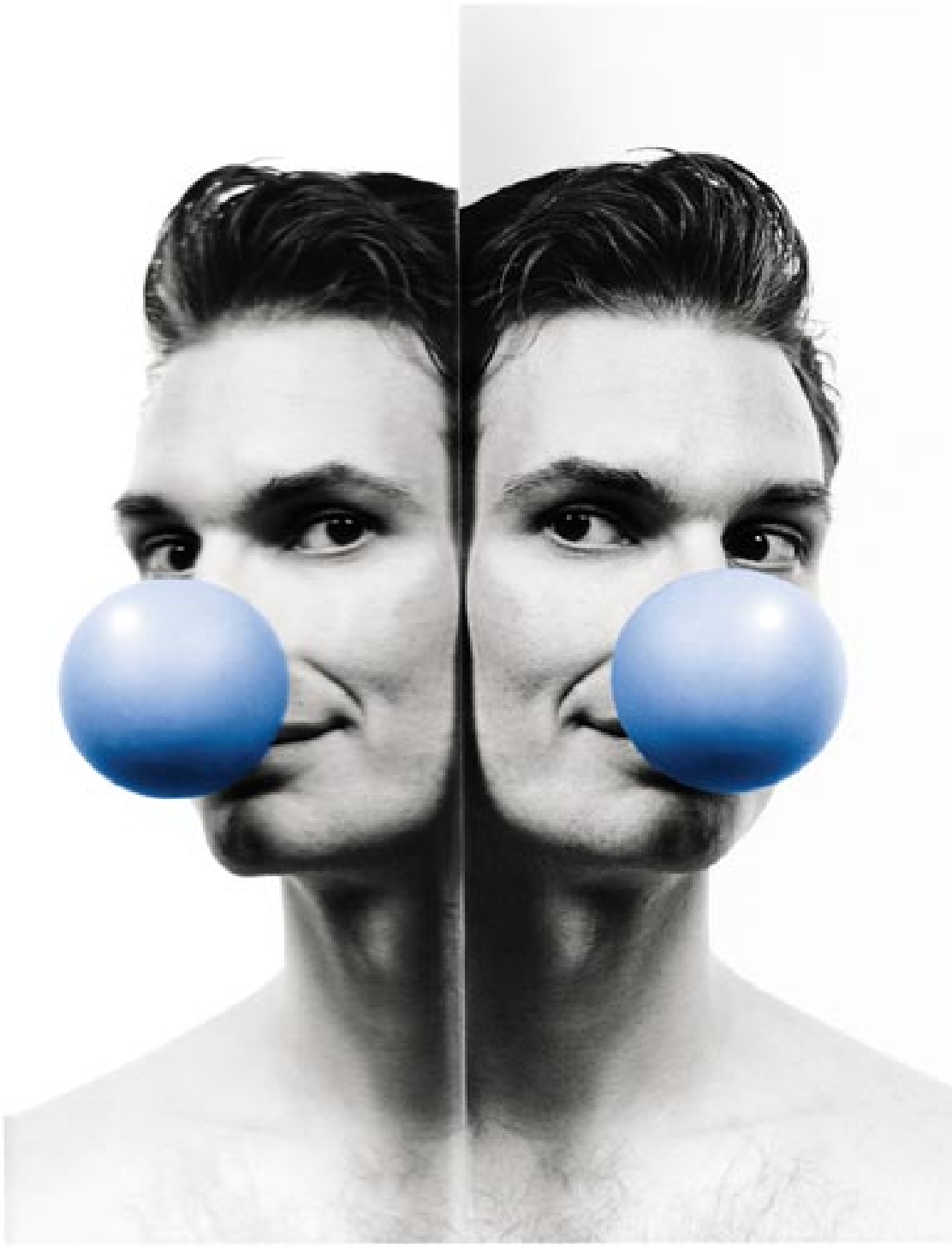
Z technického hľadiska integritu zabezpečujú matematické výpočty vytvárajúce tzv. „odtlačky prstov“ daného dokumentu (nazýva sa to hodnota HASH). Takýto „odtlačok prsta“ je unikátnym pre konkrétne množstvo informácie. Aj pri akejkoľvek malej zmene sa zmení aj „odtlačok prsta“. Takýto „odtlačok prsta“ má vždy rovnakú veľkosť, či sa už jedná o dokument s niekoľkými riadkami alebo 500-stranovú správu.

Integrita znamená, že nedošlo k pozmeneniu dát kýmkoľvek, a zároveň, že nedošlo k zmene v dôsledku poruchy pri prenose dát. Ak všetko funguje, autenticita prenášanej informácie je garantovaná prostredníctvom digitálneho podpisu. Digitálny podpis je analógiou normálneho podpisu perom na dokumente. Ak je prítomný digitálny podpis, systém predpokladá, že je všetko v poriadku.

5. nepopretie – nemožnosť popretia obdržania informácie

Nepopretie znamená, že žiadna zo strán zúčastnených na elektronickej operácii nemôže poprieť uskutočnenú transakciu. Napr. A pošle email B a objedná si kamióny Volvo. O niekoľko dní neskôr, kedže nemal dosť peňazí, to poprie. Avšak medzičasom B rozbehol operáciu dodania kamionov resp. začal s produkciou. Alebo niekto osloví banku a dá príkaz na nákup 500 akcií Ericssonu za najlepšiu možnú cenu a neskôr bude tvrdiť, že takýto príkaz v tom čase nedal, ale až o 15 min neskôr, keď cena klesla.

Kedže takéto situácie nie sú akceptovateľné, nepopretie nadobúda čoraz väčší význam v organizáciách zaoberajúcich sa elektronickým obchodovaním. Ak sa uskutoční obchod v elektronickej forme, musí mať to istú záväznosť, ako keby sa uzatváral klasickou cestou a s podpisom perom na papieri. Tento cieľ sa dosahuje pomocou elektronických podpisov, ktoré majú ešte vyššiu hladinu bezpečnosti ako ich predchodcovia, klasické podpisy na papieri. Klasický podpis je len to, čo vaše oči vidia na papieri a môže dôjsť k pozmeniu podpisu potom, ako bol vytvorený.



V elektronickom svete to nie je možné, nakoľko systém by aj pri najmenšej zmene a zásahu vyhlásil poplach.

Ak sa vrátime už k známemu príkladu Internet banky, zákazník sa prihlasuje prvýkrát vygenerovaním jednorázového hesla prostredníctvom tokenu. Následne vystaví platobný príkaz. Často sa vyžaduje „podpísanie transkacie“ prostredníctvom napr. hesla vygenerovaného tokenom alebo inou technológiou.

6. vystopovanie alebo elektronické overenie

Čím viac obchodných operácií sa uskutočňuje v elektronickom svete, tým viac vyvstáva potreba byť schopný vystopovať pôvod elektronického dokumentu. Dosahuje sa to niekoľkými spôsobmi, akými sú elektronické log záznamy, podpisy, elektronické overovanie a iné digitálne charakteristiky, schopné klarifikovať pôvod dokumentu alebo transakcie.

Kedy sa toto využíva? Reálnym príkladom môže byť, keď účtovník chce preskúmať peňažné účty, bezpečnosť IT alebo digitálne podpisy v prípade sporov a nejasností.

Iným príkladom môže byť trestný čin spáchany na web trhu. Ak niekto v mene iného objednal masovú produkciu, polícia si môže overiť, kto v skutočnosti túto transakciu uskutočnil, kedy a kde. Samozrejme, toto všetko kladie značné nároky na existenciu niečoho, čo by zabezpečilo elektronické vystopovanie a overovanie.

týchto 6 funkcií tvorí elementárnu základňu

Týchto 6 funkcií tvorí elementárnu základňu pre transfer akejkoľvek papierovej transakcie do elektronického sveta. Nie je nevyhnutné, aby sa v každom prípade uplatnili všetky tieto funkcie, ale skôr ich vhodná kombinácia, v závislosti od typu uskutočňovaných operácií a v závislosti od prínosov pre zákazníka.

Nie je nevyhnutné, aby súbor bol vždy zašifrovaný – ale je vždy nevyhnutné byť si istý s kým komunikujete.

Najlepším riešením je vhodná kombinácia rôznych riešení, ktoré by vytvárali nové príležitosti pre expanziu podnikania. Nákup príslušnej technológie niekedy môže pripadať ako enormná investícia. Akonáhle sa však vyjasnia nové možnosti vznikajúce vďaka vysokej bezpečnosti systému, objavia sa aj nové zdroje ziskov organizácie. Inými slovami, bezpečnosť sa veľmi rýchlo zaplatí.

Niektoré organizácie sa pozerajú na bezpečnosť IT ako na poistku - chránia sa pred nepredvídateľnými situáciami a stratami a v lepšom prípade ich to stojí len poplatky a náklady.

V skutočnosti, investície do bezpečnosti by mali byť chápané aj ako investície otvárajúce nové príležitosti na rozvoj podnikania a zvýšenie profitability organizácie.

elektronické obchodovanie a PKI

PKI sú pravdepodobne najdôležitejšie a najznámejšie 3 písmená v bezpečnom elektronickom podnikaní. PKI je skratkou pre Public Key Infrastructure, čo v preklade znamená infraštruktúru verejných kľúčov využívaných na zabezpečenie všetkých 6-tich funkcií spomínaných v predchádzajúcom texte.

V podstate PKI je systém na vytvorenie digitálnej identity dostatočne bezpečným spôsobom na to, aby v rámci obchodovania bola nastolená dostatočná dôvera.

PKI je možné využiť na bezpečnostné funkcie v rôznych typoch aplikácií, od elektronickej pošty až po aplikácie zamerané na plánovanie zdrojov organizácie (Enterprise Resource Planning ERP) bez toho, aby koncový užívateľ musel rozumieť jeho princípu, alebo poznal jeho štruktúru a systém.

Spojením PKI a aplikácií je možné bezpečnosť administrovať z jediného bodu, tzv. Single Point of Administration. Tým sa značne uľahčí úloha užívateľa, ktorému stačí pamätať si jedno heslo na prístup k jeho aplikáciám (Single Sign On). Ďalším dôsledkom sú nízke náklady na administráciu externých aj interných užívateľov.

Príklady typických aplikácií:

- **Bezpečný E-mail.** Čoraz väčší podiel informácií je prenášaný elektronickou poštou a je nevyhnutné zabezpečiť dôvernosť, integritu a overenie pôvodu týchto dát, a to tým viac, čím väčšia je hodnota informácií prenášaných po Internete.
- **Bezpečný klient.** Pre väčšinu ľudí je zrejmé a logické uzamykanie a bezpečné uloženie dokumentov obsahujúcich citlivé a tajné informácie. Napriek tomu, informácie uložené v digitálnej podobe sú často ponechané voľne a bez ochrany. Bezpečnosť klienta na báze využitia PKI využíva rôzne typy transparentného a automatického šifrovania a dešifrovania informácii lokálne ukladaných u klienta.

- **Bezpečné služby na www.** Čoraz viac organizácií na distribúciu informácii, produktov a služieb využíva Internet. Avšak na využitie maximálneho potenciálu Internetu a udržanie vysokej bezpečnosti, ponúkané služby musia mať zabudovanú bezpečnosť.
- **Bezpečná komunikácia.** Prostredníctvom bezpečných virtuálnych privátnych sietí (Secure VPN) sa organizácie môžu efektívne spájať a komunikovať cez Internet bez ohľadu na geografickú lokalitu. VPN riešenie na báze PKI ponúkajú autentifikáciu, dôvernosť a integritu potrebné na vybudovanie bezpečných intranetových a extranetových riešení.

základy šifrovania, kľúče a certifikáty

Existujú dvá základné spôsoby šifrovania. Symetrické šifrovanie, ktoré na zašifrovanie a dešifrovanie používa ten istý kľúč. Nevýhodou je, že pri komunikácii s viacerými subjektami pri používaní a zdielaní toho istého kľúča primerane klesá bezpečnosť. Znamená to, že pre každé spojenie potrebujete jednu sadu kľúčov a pokiaľ by ste navzájom komunikovali 5-ti, potrebujete 25 kľúčov - čo nie je síce nemožné, ale ani nie jednoduché. Prirodzene, pri narastajúcom počte prepojení sa takéto riešenie stáva nepraktické. Tu prichádza k slovu asymetrické šifrovanie. Asymetrické šifrovanie využíva pár kľúčov, z ktorých je jeden verejný (Public) a jeden tajný - privátny (Secret). Spolu vytvá-rajú tzv. pár kľúčov. Informácia zašifrovaná jedným z týchto kľúčov môže byť dešifrovaná len druhým kľúčom a vice versa.

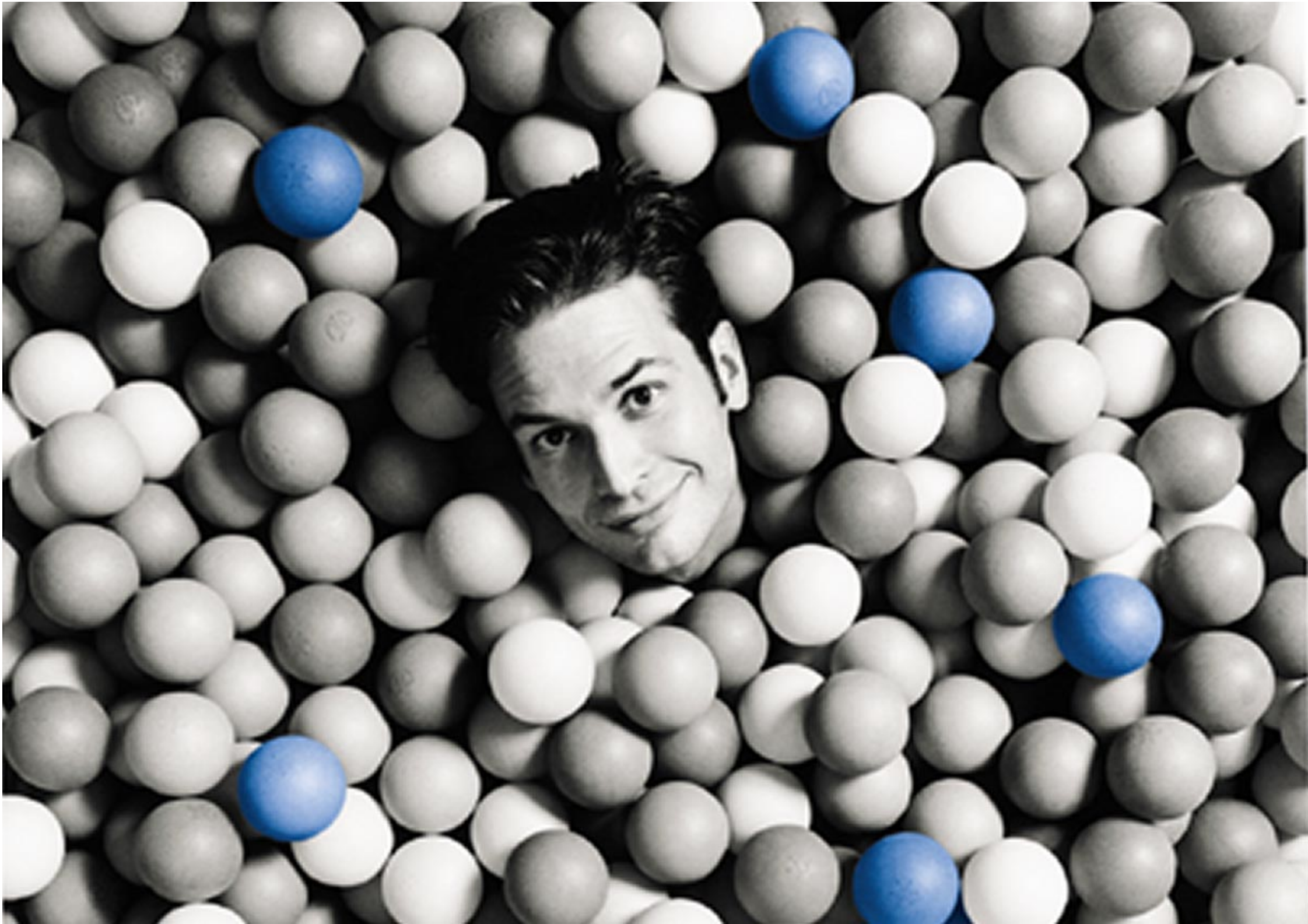
V čom je teda výhoda? Jednoducho v tom, že verejný (Public) kľúč môžem voľne distribuovať a zaslať každému koho poznám, ale aj úplne cudzím subjektom. Zároveň druhý kľúč (Secret) ostáva utajený a poznám ho len ja. Nakoľko každý má prístup k môjmu verejnému kľúču, môžu mi posielať správy zašifrované týmto kľúčom. Len ja ich môžem dešifrovať, pretože vlastním zodpovedajúci privátny kľúč - nikto iný. Používaním verejného a privátneho kľúča je vyriešený problém výmeny a správy kľúčov.

Zároveň je potrebné riešiť aj certifikáciu kľúčov voľne dostupných cez Internet. Ďalej je dôležité byť schopný overiť, kto vlastne správu zašifroval. Tu nastupuje tretí subjekt – certifikačná autorita (CA), ktorá vystavuje certifikát obsahujúci kľúč a garantuje komu patrí a dokedy platí. CA k certifikátu pridáva vlastný elektronický podpis na zabezpečenie integrity certifikátu (t.j. že ho nikto nemôže zmeniť). Analógiou može byť ID karta s hologramom alebo vodotlačou.

CA odosiela certifikát na verejne dostupnú web stránku napojenú na elektronický adresár. Ak A chce komunikovať s B, A sa spojí s informačnou službou a vyžiada si certifikát patriaci B. Po obdržaní certifikátu je schopný odoslať správu pre B bezpečným spôsobom. Na druhej strane, B je schopný si overiť, že správa prišla naozaj od A.

Cela táto procedúra sa pochopiteľne odohráva transparente pre koncového užívateľa.

V niektorých prípadoch, organizácie vydávaju certifikáty pre svojich obchodných partnerov a zákazníkov. Inou možnosťou je vydávanie certifikátov vládou alebo štátnou administratívou. Len účastníci danej bezpečnostnej domény si budú dôverovať navzájom. Participant nemôže dôverovať hocikomu, ale len tým, ktorí sú certifikovaní tou istou CA. Samozrejme bezpečnostné domény môžu využívať tzv. cross certifikáciu a tým vytvoriť dôveru medzi užívateľmi v jednotlivých doménach.



Desať prikázaní pre bezpečné elektronické podnikanie

1

Otázky bezpečnosti IT musí riešiť management.

2

Dôvera je základom dobrého obchodu.

3

Bezpečnosť je nutne integrovať hneď od začiatku.

4

Pre užívateľa je potrebné zabezpečiť jednoduchosť.

5

V novom prostredí sa musí zachovať úroveň bezpečnosti

6

Zistite si, s kým podnikáte

7

Bezpečnostná politika musí byť definovaná v každej organizácii

8

Vytvorte prostredie na tesný kontakt so zákazníkmi

9

Bezpečnosť je investícia, nie náklad

10

Vyvážte hodnotu transakcie a hladinu bezpečnosti

www.protectdata.sk
www.protectdata.cz

Bezpečnosť IT - jednoducho protect data